The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
09/21/2016

SUBJECT:
Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Apple macOS Server, macOS Sierra, iCloud and Safari, the most severe of which could allow for arbitrary code execution. Apple macOS Server is the operating system utilized by Macintosh servers. Apple macOS Sierra is the operating system utilized by Macintosh computers. Apple iCloud is an online storage service. Apple Safari is a web browser available for OS X, iOS and Microsoft Windows. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code with kernel privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- macOS Server prior to 5.2
- macOS Sierra prior to 10.12
- Safari prior to 10
- iCloud for Windows prior to 6

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Apple has released patches for multiple vulnerabilities that have been discovered in Apple products. The most severe of these vulnerabilities could result in arbitrary code execution. Details of these vulnerabilities are as follows:

- An issue existed in the handling of the HTTP_PROXY environment variable. (CVE-2016-4694)
- RC4 was removed as a supported cipher. (CVE-2016-4754)
- Multiple issues in PHP, the most significant of which may lead to unexpected application termination or arbitrary code execution. (CVE-2016-5768, CVE-2016-5769, CVE-2016-5770, CVE-2016-5771, CVE-2016-5772, CVE-2016-5773, CVE-2016-6174, CVE-2016-6288, CVE-2016-6289, CVE-2016-6290, CVE-2016-6291, CVE-2016-6292, CVE-2016-6294, CVE-2016-6295, CVE-2016-6296, CVE-2016-6297)
- A memory corruption issue was addressed through improved memory handling. (CVE-2016-4697)
- A null pointer dereference was addressed through improved input validation. (CVE-2016-4696)
- A validation issue existed in the task port inheritance policy. (CVE-2016-4698)
- Multiple memory corruption issues were addressed through improved input validation. (CVE-2016-4699, CVE-2016-4700)
- A validation issue existed in the handling of firewall prompts. (CVE-2016-4701)
- A memory corruption issue was addressed through improved memory handling. (CVE-2016-4779)
- A memory corruption issue was addressed through improved memory handling. (CVE-2016-4702)
- A memory corruption issue was addressed through improved input validation. (CVE-2016-4703)
- An input validation issue was addressed through improved memory handling. (CVE-2016-4706)
- An issue existed in Local Storage deletion. (CVE-2016-4707)
- An input validation issue existed in the parsing of the set-cookie header. (CVE-2016-4708)
- An input validation issue existed in corecrypto. (CVE-2016-4711)
- An out-of-bounds write issue was addressed by removing the vulnerable code. (CVE-2016-4172)
- A user with screen sharing access may be able to view another user's screen (CVE-2016-4713)
- Multiple issues in curl (CVE-2016-4606)
- An issue existed in the handling of the .GlobalPreferences file. (CVE-2016-4715)
- An access issue existed in diskutil. (CVE-2016-4716)
- A resource management issue existed in the handling of scoped bookmarks. (CVE-2016-4717)
- A buffer overflow existed in the handling of font files. (CVE-2016-4718)
- A spoofing issue existed in the handling of Call Relay. (CVE-2016-4722)
- Multiple memory corruption issues were addressed through improved memory handling. (CVE-2016-4723)
- A null pointer dereference was addressed through improved input validation. (CVE-2016-4725)
- A memory corruption issue was addressed through improved memory handling. (CVE-2016-4726)
- A memory corruption issue was addressed through improved memory handling. (CVE-2016-4727)
- A timing side channel allowed an attacker to determine the existence of user accounts on a system. (CVE-2016-4745)
- A parsing issue in the handling of directory paths was addressed through improved path validation. (CVE-2016-4771)
- A lock handling issue was addressed through improved lock handling. (CVE-2016-4772)

- Multiple out-of-bounds read issues existed that led to the disclosure of kernel memory. These were addressed through improved input validation. (CVE-2016-4773, CVE-2016-4774, CVE-2016-4776)
- A memory corruption issue was addressed through improved memory handling. (CVE-2016-4775)
- An untrusted pointer dereference was addressed by removing the affected code. (CVE-2016-4777)
- Multiple memory corruption issues were addressed through improved memory handling. (CVE-2016-4778)
- Multiple memory corruption issues existed in libarchive. (CVE-2016-4736)
- Multiple memory corruption issues were addressed through improved memory handling. (CVE-2016-4658, CVE-2016-5131)
- A memory corruption issue was addressed through improved memory handling. (CVE-2016-4738)
- Applications using VMnet.framework enabled a DNS proxy listening on all network interfaces. (CVE-2016-4739)
- A state management issue existed in NSSecureTextField, which failed to enable Secure Input. (CVE-2016-4742)
- An issue existed in the parsing of environment variables. (CVE-2016-4748)
- A memory corruption issue was addressed through improved memory handling. (CVE-2016-4750)
- A resource management issue existed in the handling of key derivation. (CVE-2016-4752)
- A validation issue existed in signed disk images. (CVE-2016-4753)
- A permissions issue existed in .bash_history and .bash_session. (CVE-2016-4755)
- A type confusion issue was addressed through improved memory handling. (CVE-2016-4709, CVE-2016-4710)
- Multiple validation issues were addressed through improved input sanitization. (CVE-2016-4618)
- A state management issue existed in the handling of tab sessions. (CVE-2016-4751)
- A parsing issue existed in the handling of error prototypes. (CVE-2016-4728)
- A permissions issue existed in the handling of the location variable. (CVE-2016-4758)
- Multiple memory corruption issues were addressed through improved memory handling. (CVE-2016-4611, CVE-2016-4729, CVE-2016-4730, CVE-2016-4731, CVE-2016-4734, CVE-2016-4735, CVE-2016-4737, CVE-2016-4759, CVE-2016-4762, CVE-2016-4766, CVE-2016-4767, CVE-2016-4768, CVE-2016-4769)
- Safari's support of HTTP/0.9 allowed cross-protocol exploitation of non-HTTP services using DNS rebinding. (CVE-2016-4760)
- Multiple memory corruption issues were addressed through improved state management. (CVE-2016-4733, CVE-2016-4765)
- A certificate validation issue existed in the handling of WKWebView. (CVE-2016-4763)

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code with kernel privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by Apple to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user to diminish the effects of a successful attack.
- Remind users not to download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:
Apple:
https://support.apple.com/en-us/HT207147
https://support.apple.com/en-us/HT207157
https://support.apple.com/en-us/HT207170
https://support.apple.com/en-us/HT207171

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4606
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4611
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4618
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4658
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4694
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4696
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4697
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4698
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4699
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4700
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4701
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4702
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4703
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4706
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4707
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4708
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4709
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4710
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4711
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4712
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4713
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4715
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4716
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4717
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4718
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4722
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4723
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4724
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4725
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4726
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4727
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4728
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4729

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4730
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4731
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4733
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4734
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4735
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4736
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4737
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4738
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4739
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4742
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4745
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4748
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4750
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4751
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4752
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4753
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4754
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4755
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4758
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4759
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4760
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4762
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4763
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4765
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4766
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4767
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4768
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4769
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4771
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4772
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4773
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4774
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4775
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4776
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4777
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4778
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4779
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5131
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5768
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5769
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5770
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5771
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5772
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5773
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6174
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6288
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6289
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6290

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6291
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6292
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6294
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6295
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6296
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6297